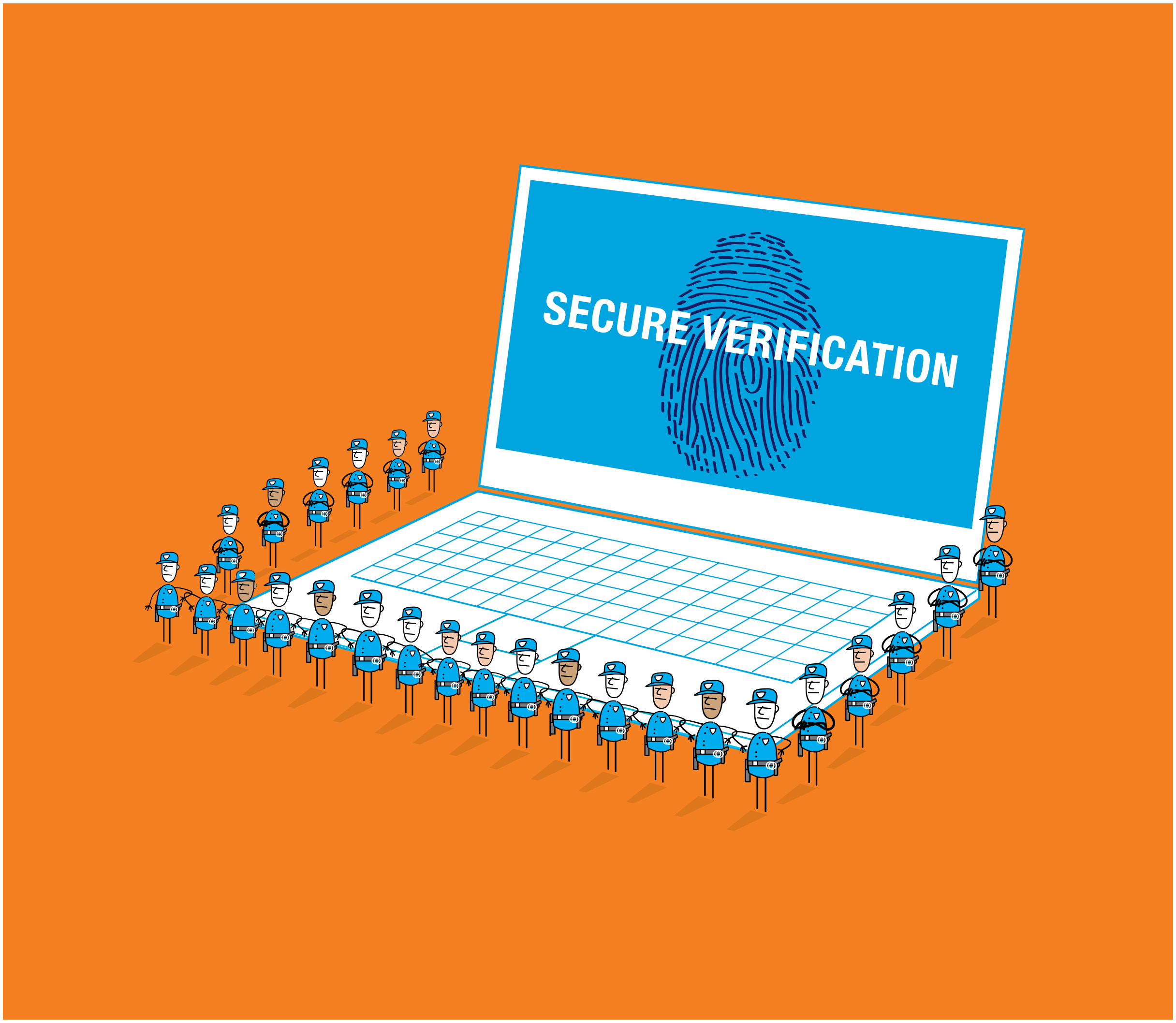
PROTECTING OUR CYBER FUTURE

Be proactive before it's too late

CHARTERED ACCOUNTANTS
AUSTRALIA + NEW ZEALAND



future [inc]
A PLAN FOR AUSTRALIA + NEW ZEALAND'S PROSPERITY

charteredaccountantsanz.com/futureinc

America’s economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable internet.

Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the internet remains an engine for economic growth and a platform for

THE FREE EXCHANGE OF IDEAS.

PRESIDENT OBAMA
ON FEBRUARY 12, 2013, PRESIDENT OBAMA SIGNED EXECUTIVE ORDER 13636, *IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY.*

future[inc]

A PLAN FOR AUSTRALIA + NEW ZEALAND'S PROSPERITY

FOREWORD

With what seems like an unstoppable growth in technology, now more than ever, we are connected on a global scale. With this growth it has also become increasingly important to pay attention to cyber security, but even more important to address how we curb cyber threats and crime. With the increased volume and sophistication of cyber threats, a bigger discussion needs to take place; we need to be proactive rather than reactive. Cyber security is more than a security issue; it is also a strategic issue.

The latest in our ***future*[inc]** series discusses the threat of cyber security in the Asia Pacific region and provides insight into how to take traditionally reactive approaches and turn them into proactive engagements.

This is a discussion that is taking place all over the world. Australia and New Zealand can no longer afford to be complacent about this issue. I'd like to thank the team at Deloitte for contributing to this paper. I would also like to thank the many individuals involved in the production and consultation of this paper. This is one piece of a larger discussion taking place as part of our ***future*[inc]** series.

I hope you enjoy our thinking and I encourage you to join the conversation to help shape the future of Australia and New Zealand.

M. Ashton

Mel Ashton FCA
President designate

CHARTERED ACCOUNTANTS
AUSTRALIA + NEW ZEALAND

charteredaccountantsanz.com/futureinc

CONTENTS

SUMMARY

CYBER LANDSCAPE

- Cyber attacks have evolved from worms to brick attacks – reflecting the sophistication of the cyber terrorist.
- Businesses are vulnerable, ignore the threat at your peril.
- Attackers could be the state staying ahead of competitor nations; hacktivists who want to voice their cause publicly; or, criminals who just want the money.
- Attackers are no longer simply after credit card data – they want whatever makes an organisation competitive and destroys the opposition.
- Cyber terrorists are well resourced, highly organised and capable of innovating faster than you can.
- The Domino Effect – once you're a target, everything else can come tumbling down, from share price to reputation.

IMPACT ON THE BOARD AND EXECUTIVES

- Cyber security isn't just an IT issue – the broader C-suite must be engaged before the organisation can become more secure.
- The role of the Chief Information Officer is changing in part because of cyber threat.
- The CIO needs to align IT and security concerns with the overall business goals.
- Cyber threat needs to move up the boardroom agenda.

ORGANISATIONAL PREPAREDNESS

- Plan for the worst case scenario. Knee jerk responses can taint a security incident.
- Be prepared, with clear communications, and an escalation process.
- Ensure the admin is watertight – store logs and consider engaging a forensic agency.
- Proper preparation is essential – conduct scenarios to make sure systems work.
- Ensure a cyber-aware security culture.
- Ensure you insure against attacks.

ROLE OF REGULATORS

- Having cyber security strategies is a good start, but both Australia and New Zealand's regulators need to address the cyber preparedness of their regulated communities.
- No current attempt across states and territories to manage regulations ... potentially leaving businesses vulnerable.
- Internationally, regulators actively meet chief executives to discuss cyber threats and preparedness.
- The International Organisation of Securities Commissions (IOSCO) said that regulators are planning to launch a global toolbox in 2015 to help with cyber attack preparedness.

INTRODUCTION

The annual global cost of cyber attacks to business and individuals is around USD $133 billion. In Australia it's just over $1 billion and in New Zealand around $625 million.* No matter how you look at it, cyber security has to become one of the top issues that Chief Executives address with their Boards, and with the Executive Team.

In the Asia Pacific region, organisations generally feel immune from attack because of the lack of cyber-crime statistics which is helpful when committing budget, and making business decisions. Alongside the lack of data, our legislative framework has had historically limited regulatory options with which to penalise organisations. The lack of data and threat of penalty means that cyber security is often way down the boardroom agenda, and worse, is often ignored altogether.

* annual Norton cybercrime report from security firm Symantec.

These new vulnerabilities mean cyber security can no longer be confined to the IT department. **A CYBER-ATTACK CAN DAMAGE A BUSINESS IN MANY DIFFERENT WAYS**.

Recently passed amendments to the Australian Privacy Act, 1988 are a step in the right direction. They carry enough weight so that organisations take notice. One significant amendment includes the ability for the Privacy Commissioner to act independently and conduct investigations which carry significant pecuniary penalties.

Another change to the legislation allows the Privacy Commissioner to initiate an investigation. Previously a complaint would need to be lodged in order for the Commissioner to start an investigation.

From an organisation's perspective, security often sits with the IT Department where the value of investment in gateways, firewalls, intrusion prevention systems, anti-virus and other security armoury is well understood. But these measures are now considered the bare minimum.

With the ever increasing sophistication of mobile devices and technology, organisations have an ever-expanding online footprint. Technology is online. Employees work online. Customers and suppliers do business online. Consequently, an organisation's reputation can be made or broken online.

This means that cyber security is no longer an issue that can be resolved with more investment in software and equipment. Today's cyber attacks are increasingly sophisticated and complex, driven by elaborate and resilient professional groups that innovate faster than their targets.

The motivation for cyber attacks have also become more complex. A broader range of hackers are no longer just after customers' credit cards – they're after intellectual property and information that can be monetised or used to support their objectives.

Some want to damage your brand, full stop. Some want revenge. Others are simply having fun.

All this means that cyber security can no longer be confined to the IT Department. With an organisation's reputation, share price, goodwill and trust at risk, cyber security needs to be a whole of organisation issue. The key consideration is whether an organisation's cyber security measures are capable of preventing attacks rather than just complying with industry best practice. An organisation with a mature and effective approach to cyber security rarely settles for compliance.

This paper serves as a guide to thinking about dealing with a cyber threat and encourages business to move from being reactive to being proactive before it's too late.

CYBER LANDSCAPE

EVOLUTION OF CYBER THREATS

Cyber threats are not a new phenomena. However, the types of attacks and methods have evolved greatly. Almost two decades ago the talk was of worms, viruses and DDoS (distributed denial of service) attacks. They were often the work of individuals and pranksters, usually programmers who were looking for notoriety or to gain recognition for their programming skills. The result of these early cyber threats was disruption. Some of these early threats included CIH computer virus and the slammer worm.

FIGURE 1: MAJOR CYBER ATTACKS

DATE	COUNTRY	EVENT
OCTOBER 2014	**USA**	76 million households were affected by a cyber attack on a global US based bank. Customer data was stolen including names, addresses and phone numbers.
SEPTEMBER 2014	**USA**	Home improvement and construction products retailer listed on the NYSE announced 56 million customer debit and credit card details were at risk after custom malware infiltrated the company's computer system.
JUNE 2014	**France and Belgium**	Large global pizza chain held to ransom over 600,000 Belgian and French customer records. In exchange for personal data a ransom of $40,000 was demanded. The organisation refused to pay the ransom but the data was never released.
MAY 2014	**USA**	Multinational ecommerce company revealed hackers managed to steal personal records of 2.33 million users. Usernames, passwords, phone numbers and addresses compromised. Later revealed to be a hacktivist attack.
MAY 2014	**Australia**	'Oleg Pliss' locks the accounts of a number of iPhone users in Australia and demands a ransom.
DEC 2013	**USA**	Several major retailers attacked stealing customer data. This included 40 million payment card numbers from one major retailer alone.

Cyber threats began to evolve around ten years ago from disruptive events to cyber crime. The instigators have evolved from pranksters to organised criminal gangs, nation-states and hacktivist groups. These new forms of cyber crime were the earliest attempts at malware and were done largely for monetary gain. One of the earliest malware attacks was Mydoom which spread via spam and stole email addresses to further proliferate. The infected machines would be part of a botnet. Cyber crime has continued to evolve from the use of malware to attacking trusted digital communication technologies and now to digital certificates. Ransomware and cyber kidnapping has increased where criminal gangs gain control of information critical to an organisation or government and demand a ransom. Figure 1 shows some of the major cyber attacks over the past 12 months.

The sophisticated methods employed by cyber criminals has coincided with megatrends around globalisation and economic interconnectedness and the ever increasing role of technology, to form a powerful tsunami where cyber threats are one of the biggest threats to the global economy.

Cyber threats have turned into mega breaches with breaches growing in number and scale. The cyber attacks have not only continued to rise in number but they are also more targeted. The Symantec Corporation's Internet Security Threat Report 2014 stated the most targeted attacks were against governments and the services industry, however, it also identified mining and manufacturing industries as being at risk.

CYBER JARGON BUSTER

TROJAN HORSE

Trojan horses are software programs that masquerade as regular programs but do malicious things to your computer. Unlike viruses Trojan horses do not replicate themselves.

RANSOMWARE

Is a type of malware which prevents access to a system until a ransom is paid. The CryptoLocker ransomware stole around USD $3 million before it was taken down.

BOTNET

Formed from the 'robot' and 'network' botnets can be used for good and bad. For bad (where we're focussing) botnets can attack computers when security has been breached and can send out spam emails.

WORMS

Self-reliant program which replicates over a network using protocols. The Code Red 11 worm infected more than 259,000 systems in less than 14 hours.

VIRUSES

Can hide in computer memory and attached to files where it can reproduce. It can change its footprint too which makes it hard to locate.

HACKTIVIST

Not a British rap metal band from Milton Keynes, but a hacker who hacks to disrupt and highlight political or social causes.

MYDOOM

Is a worm designed to send junk email through infected computers and includes the message "Andy, I'm just doing my job, nothing personal, sorry".

MALWARE

Malicious software (also known as badware) includes worms and viruses. It's any software that's designed to disrupt or is hostile.

FIGURE 2: ORGANISATIONS BEHIND CYBER SECURITY THREATS

State-sponsored	Hacktivist	Criminal
Intellectual property Information Warfare Disruption	Sensationalism Disruption Environmentalism Social impact	Monetisation Data Intellectual property Financially motivated

Loss of reputation and trust

KNOW YOUR ENEMY

Understanding that the landscape has changed is the first step in illustrating the significant importance of cyber security. When educating stakeholders and business leaders, it helps to paint a picture of those behind the threats.

YOUR ADVERSARY

The organisation behind a cyber-threat is often well resourced – even potentially sponsored by a nation state – and runs rigorous multi-layered campaigns across many years. It is also highly organised, professional and capable of innovating faster than you can.

For example, a cyber-crime cartel might target an organisation's network to sell access onto another organisation that manages deeper security layers.

TACTICS

Cyber attackers no longer use the 'smash and grab' approach. Many maintain presences for years and aim to operate well below the security radar of their target organisations.

Traditional security controls such as firewalls, antivirus programs, and intrusion detection systems become increasingly less effective as attackers develop innovative new techniques to evade them.

Attackers are also no longer simply after credit card data. Instead, they're looking for whatever makes an organisation competitive, for example, research and development information, customer data, intellectual property and marketing strategies. The motivations behind cyber-crime are varied, but often fall into one of three broad categories defined by those responsible for the threat, see Figure 2.

STATE-SPONSORED

State-sponsored espionage has become more common as a strategy to stay a step ahead of other nations, with numerous recent public disclosures about the extent of governmental intervention.

State-level cyber threats are often characterised by extremely advanced technologies and methods, which makes them expensive and difficult to evade.

HACKTIVISTS

Hacktivists are organised groups of politically motivated individuals who feel a need to voice their cause publicly by targeting the reputation of organisations that do not yield to their demands.

They often launch attacks to gain publicity. Accordingly, they present more of a risk to an organisation's brand and reputation than to its financial information or intellectual property.

CRIMINALS

The goal for cyber-criminals is to monetise that which organisations or individuals value. Cyber criminals use sophisticated methods and tools to tailor attacks to organisations and increase their success rates.

Organised cyber-crime is increasingly the factor most responsible for the growing risk gap in organisations, as cyber criminals become smarter and more resourceful in their quest to create chaos. The effect of cyber-crime is also complicated by the difficulty many organisations have when it comes to hiring and retaining experienced cyber security individuals.

Additionally, accidental loss or system glitches exacerbate the effects of the three main threat sources, and accounted for 57% of data breaches in Australia in 2013 alone.

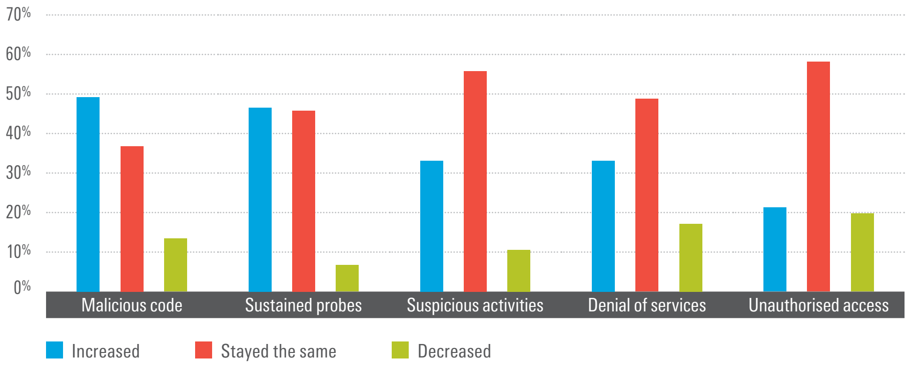
EVOLVING THREATS

The cyber security landscape is constantly evolving, and organisations need to have a strategy in place to address their security position.

What is a threat now can rapidly change, and the security strategy needs to accommodate this movement. Figure 3 provides projections on where cyber threats are likely to come from according to the Ponemon Institute 2014 Cost of Data Breach Study: Global Analysis.

FIGURE 3: CHANGES IN SECURITY THREATS OVER THE FORTHCOMING YEAR (2015)

Consolidated view (n=314)



SOURCE: Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis.*

LOOKING AHEAD

While current cyber threats will continue to evolve, new forms of threats will also develop. Here are three cyber threats that will continue to grow.

1. MOBILE MALWARE

2013 saw cyber attacks on mobile devices. It is predicted that this will continue to grow in terms of both the sophistication of the attacks but also the volume of attacks.

'Oleg Pliss' ransomware was used to target mobile phone users in Australia in 2014. Device owners could only get their device unlocked once they paid a ransom. This is an early example of the move towards targeting mobile devices.

2. CYBER KIDNAPPING AND RANSOMWARE

Cyber kidnapping and ransomware is expected to increase. As both organisations and individuals are heavily dependent on technology and online capabilities, control of these capabilities is open to exploitation. The 'CrypoLocker' virus in 2013 was a very recent example of the potential of ransomware. Although these attacks have been limited, they are expected to grow. The payment of ransoms will be aided by the use of digital currencies which gives cyber criminals the ability to receive payments anonymously.

3. BRICK ATTACKS

Stealing data is not the only risk for organisations. In brick attacks cyber criminals destroy information rather than just steal it. For example, accounts could be completely erased from a bank's records. In 2013 the world's largest oil company was hit with a brick attack that destroyed 30,000 computers.

Most cyber attacks are against **GOVERNMENTS AND THE SERVICE INDUSTRY**, and mining and manufacturing industries are at risk.

THE IMPACT OF A CYBER SECURITY BREACH

Hackers, viruses and cyber terrorists are just a few of the potential threats actively seeking to exploit your system's vulnerabilities. Other threats – such as human error – are less malicious but can be just as dangerous.

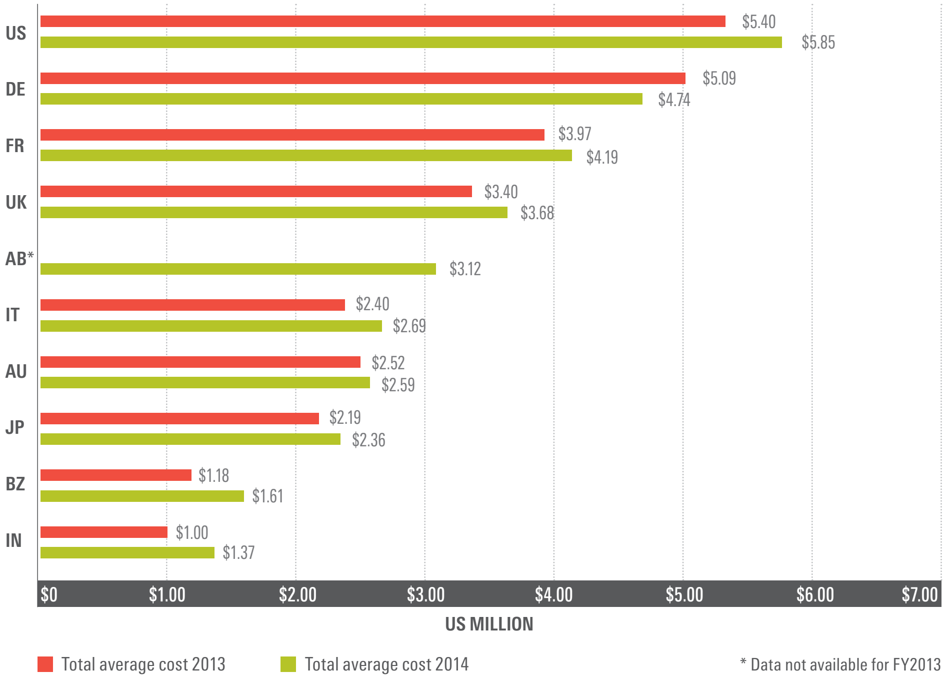
The consequences of failures arising from these threats range from embarrassing to life-threatening. Once attackers find what they're looking for, the fallout can extend from brand damage and loss of revenue to lower share prices and more regulatory scrutiny. The costs associated with investigation, remediation, fraud, litigation and the associated penalties are typically high, see Figure 4.

The most recent report by the Ponemon Institute found the average total organisational cost for a data breach is increasing in most countries. In Australia it is now USD $2,59 million.

DETECTION AND ESCALATION COSTS

Detection and escalation costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. These are the costs associated with responding to breaches.

FIGURE 4: THE AVERAGE TOTAL ORGANISATIONAL COST OF DATA BREACH OVER TWO YEARS



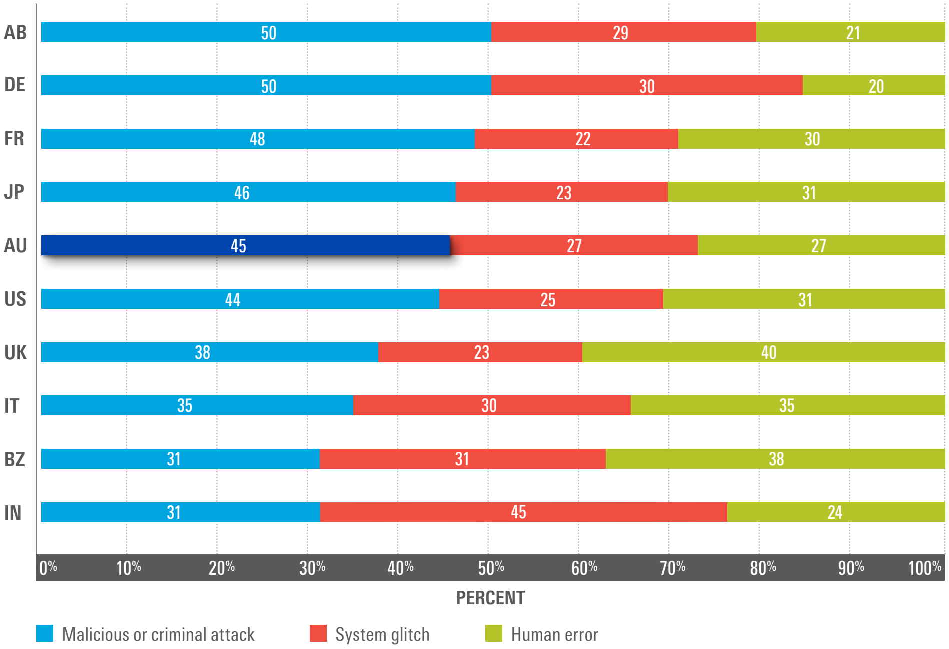
* Data not available for FY2013

SOURCE: Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis.*

CAUSE OF DATA BREACH

The information in Figure 5 highlights the likelihood of a malicious attack. Australia has been identified as having a 45% attribution to malicious attack as the root cause of data breaches. The remaining root causes are results of system glitches and human error.

FIGURE 5: DISTRIBUTION OF THE BENCHMARK SAMPLE BY ROOT CAUSE OF THE DATA BREACH



SOURCE: Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis.*

One US based retailer had an estimated **100 MILLION POTENTIAL CREDIT CARD BREACHES**.

THE DOMINO EFFECT

Recent large-scale security incidents have shown that security breaches can have a range of adverse consequences.

In 2013, a major global retailer was hit with a cyber-attack that cost millions of dollars and drastically affected its share price. Although the retailer had invested over $100 million in cyber security measures, it had failed to establish end-to-end monitoring and response, and could not respond quickly enough when hackers targeted its Point of Sale (PoS) system during an intensely busy period.

The 2013 breach exposed 40 million customer payment card details and precipitated a domino effect that caused difficulties beyond the IT department, including repayments to cardholders, regulatory fines, loss of share value and significant legal action.

Then, in 2014, another major retailer was affected by a variant of the same malware, This particular variant, which was highly customised, involved skimming customers' credit card details as they were processing their purchases at the self-service PoS checkouts. This breach went unnoticed for almost 5 months, and is estimated to be the second largest ever known breach to occur with an estimated 70 million customer details stolen across the US and Canada. The retailer estimated the investigation, credit monitoring service, call center staffing and other steps would cost a total of USD $62 million, offset by USD $27 million which it expects to be reimbursed by its insurance.

Research has identified one US based retailer who had an estimated 100 million potential credit card breaches.

There are other costs which are difficult to quantify, including the affected customers' loss of time, from being disadvantaged whilst awaiting to receive their new credit cards, checking statements for fraudulent activity and the customers' financial institution costs to press and re-issue new credit cards to prevent future fraudulent charges.

Closer to home in October 2012, a New Zealand Government Agency experienced a breach on internet kiosks accessible by the public for job searches. The kiosks were actively connected to the NZ Government Agency corporate network which provided access to client information including recorded conversations and active investigations. This resulted in several senior level sackings of executives in the organisation, and a major dent it the agency's reputation.

As well as focusing on regulatory compliance and investment in cyber security, organisations should identify their greatest points of vulnerability and ensure these are secure.

However, the risk of these outcomes can be greatly reduced with the right procedures, technologies and rigorous attention to detail through regular testing.

Effective cyber security has as much to do with good practice and common sense as compliance. Focusing too closely on IT alone can easily result in unauthorised data loss or exposure.

IMPACT ON THE BOARD AND EXECUTIVES

ELEVATING THE CONVERSATION WITH THE BOARD AND EXECUTIVES

It can be difficult to communicate the scale and importance of cyber security to business leaders. CIOs should use the following four steps to position cyber security as an ongoing conversation within the organisation, and to gauge the effectiveness of existing cyber security measures.

> Cyber security is not just the IT department's challenge – **THE BROADER C-SUITE MUST BE ENGAGED** before the organisation can become more secure.

1. BE PREPARED

Accept that you will be hacked and should be prepared.

2. SET THE BAR

Protect what matters most in terms of confidentiality, integrity and availability, and focus spend in these areas.

3. GET THE BASICS RIGHT

It's important to address all security gaps from the boardroom to the daily use of networks. Most breaches arise from a failure to cover the basics.

4. PERSONAL PROTECTION

Improve the security culture by lifting awareness of potential risks at home and at work. Ensure that the following is performed:

- Conduct security reviews regularly
- Treat outcomes as symptoms and search for the root cause
- Implement a culture of non-tolerance for security failure
- Implement culture of continual improvement.

Modernising an organisation's approach to cyber security will require changes to its strategy, people, process and technology on an enterprise scale.

THE ROLE OF THE CHIEF FINANCIAL OFFICER

Ask the right questions of the right sources. As Chief Financial Officer (CFO), the go-to sources about cyber risk are typically the CIO, the chief risk officer (CRO), and the chief information security officer (CISO). The following questions can inform the dialogue:

- How do we identify our critical assets, associated risks, and vulnerabilities?
- Do we have a well-tested incident response and communication plan?
- Do we track what information is leaving our organisation and where it is going?
- How do we know who's really logging into our network, and from where?
- Can we limit the information we voluntarily make available to a cyber adversary?
- Do our security controls cover the entire company, including subsidiaries and affiliates? (Most often the answer will be no.)

KEY CONSIDERATIONS

There are steps to take to reduce the threat of a cyber-attack. In fact, according to the Ponemon Institute's *2014 Cost of Breach: Global Analysis* study, having a strong security posture, incident response plan, and chief information security officer appointment reduced the cost of a data breach by $14.14, $12.77, and $6.59, per record, respectively.

In addition, the following actions can guide CFOs in instituting an enterprise-wide cybersecurity plan:

- **Evaluate** the existing cyber-incident response plan. Focus on the controls for the "crown jewels" and what you would do in the event of an incident. The team responsible for this should include senior management from the lines of businesses and administrative functions.
- **Identify** finance's role in cybersecurity. Work with your CIO or CISO and the business leaders to see how finance can help create the necessary culture of security and privacy. Organisations can enhance their security stance by valuing cybersecurity and the protection of privacy and viewing. Remember: 'security begins with me'.
- **Require** regular reports on security risks. These reports should be from senior management and detail privacy and security risks, based not on project status but on specific risk indicators.
- **Review** the cybersecurity budget. Many times, security budgets take a backseat to other IT or business priorities, resulting in companies being unprepared to deal with risks and attacks. An annual review of cybersecurity budgets is recommended.
- **Re-evaluate** cyber insurance. Also on an annual basis, revisit the use and need of cyber insurance.

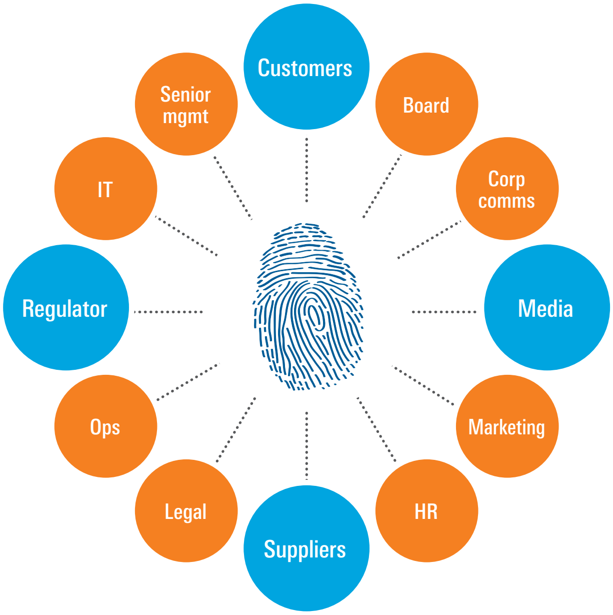


FIGURE 6: CYBER SECURITY MUST BE AN ORGANISATION-WIDE CONSIDERATION

THE NEW ROLE OF THE CHIEF INFORMATION OFFICER

IT is now viewed as one of the most effective ways to increase competitiveness, solve complex problems and deliver new revenue streams.

As a result, the Chief Information Officers' (CIO) role has evolved. Individuals who work closely with business leaders are often seen as guides, translating technology advancements into business opportunities and capabilities that can drive the organisation to meet its goals.

This means today's CIOs must adopt a range of different roles that mirror the basic corporate functions. To be successful, a CIO has to assume the perspective of:

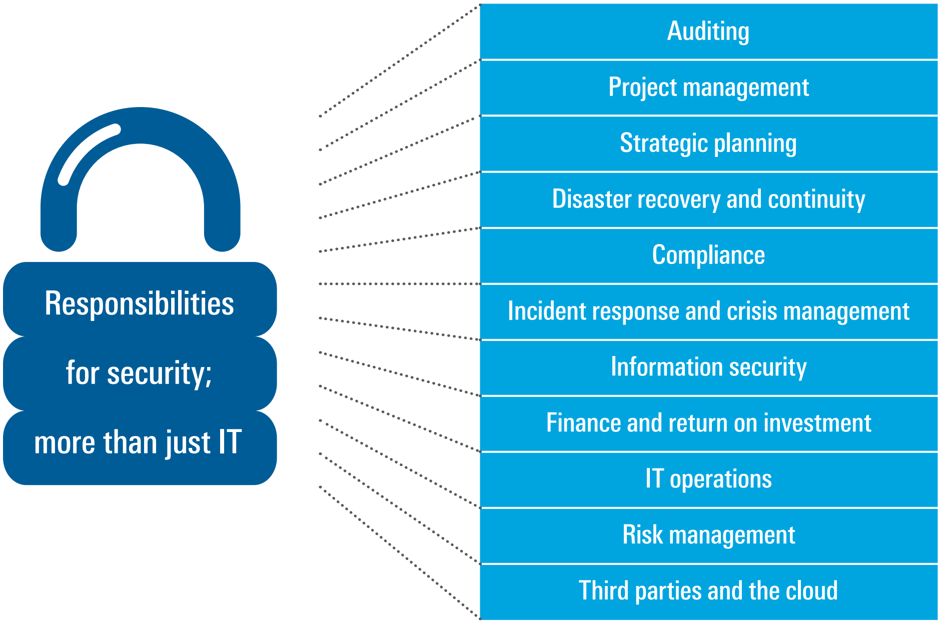
- **Strategist** – imagining and planning how IT can help clients in their efforts to be more effective
- **Technologist** – with a deep understanding of technological advancements and how they apply to the business
- **Innovator** – combining technologies and business opportunities to create practical and effective outcomes
- **Marketer** – communicating and promoting IT's capabilities and offerings to clients
- **Designer** – defining and creating service delivery processes that allow IT to keep its commitments
- **Accountant** – obtaining and managing the funding to provide new and existing services to IT clients
- **Recruiter** – enlisting, motivating, and mobilising existing and new staff
- **Revolutionary** – changing the way the business drives value.

CYBER SECURITY IS A BUSINESS ISSUE

Most executive stakeholders want things fast and cheap when it comes to IT. However, security needs to be a top priority in today's increasingly complex and connected world, and it should be the key concern across all aspects of the CIO's role.

Rather than being solely concerned with IT operations, a modern CIO must align information technology and security concerns with overall business goals. Moreover, a CIO's role is to ensure that managers throughout the organisation understand the risks and potential ramifications of a major cyber security breach.

FIGURE 7: SECURITY IS A BUSINESS-WIDE CONSIDERATION



Responsibilities for security; more than just IT

- Auditing
- Project management
- Strategic planning
- Disaster recovery and continuity
- Compliance
- Incident response and crisis management
- Information security
- Finance and return on investment
- IT operations
- Risk management
- Third parties and the cloud

ORGANISATIONAL PREPAREDNESS

CYBER PREPAREDNESS – ARE YOU READY?

IMAGINE

Your organisation has been breached. Your first response is to power the server off to stop the hacker from doing anything else.

You have just broken one of the major rules of incident response.

These are the four steps to ensure that when you are breached your response does not exacerbate the situation: plan, communicate, log and test.

PLAN

An organisation needs to plan for the worst case scenario and develop the technical and business measures to limit the potential impact to its business, by building an effective incident response plan. This will minimise the impact of a breach, reduce the visibility of the issue and ensure that the response is measured and appropriate.

Knee-jerk reactions can taint a security incident. In our imaginary scenario, turning the system off erased any traces of the incident from the operating memory of the system and the temporary files, making recovery and forensic analysis difficult. A more appropriate response would be to enact your incident response plan, which may involve disconnecting the server from the network, and contacting a computer emergency response team.

COMMUNICATE

Ensure the message is consistent from an internal and external perspective. Avoid multiple spokespeople and ensure they have a prepared script to read with no ambiguities and that technical questions are anticipated and prepared for. Determine in advance which customers you should contact, the escalation process and any liabilities that can be mitigated.

LOG

Ensure that all system and application logs are stored in their original format, are cryptographically hashed and retained to ensure that they are admissible as evidence. Only copies of the logs should be distributed to incident responders and IT teams. Engage a forensic agency to professionally review the affected systems if you do not have the internal capability.

TEST

Conduct frequent small-scale table top exercises and annual full scenario run-throughs to prove your incident response plan works, highlight any shortcomings and update the operational documentation. This familiarises the operational teams and management chain with the process which decreases incident response time and ensures that the scenario planning is taken seriously.

DOES YOUR BUSINESS CULTURE SUPPORT A SECURE ENVIRONMENT?

Culture can trump poor controls when people do the right thing despite the environment. The opposite does not hold true. A poor culture can often override controls.

Having the right cyber security culture flowing from both IT and the business is therefore important.

Five questions to test your results:

- Does the executive actively support a secure environment?
- Do we tolerate minor infringements?
- Does functionality trump security?
- Do we provide ongoing security awareness training to all staff?
- Does awareness training extend to personal and home based security?

Without a convincing argument for why they should behave in a secure way, staff tend to take the path of least resistance and follow what everyone else does. This, to a large extent, makes up the company culture (otherwise known as, 'the way we do things around here'). In contrast, a culture where security risks are taken into consideration ahead of decision-making will reduce an organisation's risk. In addition, organisations able to develop a security-minded workforce, and embed security-by-design have created a significant defence against social engineering, insider attacks and many other top security threats.

BACK TO BASICS

The Australian Defence Directorate has issued a list of the Top 4 Mitigation Strategies to protect your ICT Systems.

As a minimum, these are the basic fundamentals to be focused on. These include;

- Application whitelisting
- Patching applications
- Patching operating systems
- Minimising administrative access and privileges.

Application whitelisting is proving onerous to many but the remaining list is important.

Deloitte has concluded based on their extensive vulnerability testing, penetration testing and social engineering work that the 80:20 principle applies to cyber hacking. 80% of why they can penetrate a client's systems is because the basics are not vigorously applied.

In days gone by controls were visible to all and paper trails proved controls were operating as expected.

The controls were easily understood and visible to all from the shop floor to the boardroom. In today's environment that visibility is lost and the importance is not always understood.

When reviewing penetration test results, if issues are identified, consider if the issue is a symptom of a larger systemic issue or if the result is a one off. In Deloitte's experience it is often the former.

Hackers attack multinational ecommerce company and **STEAL PERSONAL RECORDS OF 2.33 MILLION USERS**.

IS OUTSOURCING A THREAT?

The move to outsourcing, third party joint ventures, cloud based solutions and collaborative initiatives has pierced the secure boundaries of many organisations and the notion of a secure perimeter. This can lead to the misperception of security through transfer of responsibility. Ultimately it has been proven that whoever owns the customer is always in the firing line when there is a cyber security issue. It remains fixed however, that reputational damage cannot be outsourced.

EFFECTIVENESS OF SECURITY?

The cyber security capability required needs to be determined based on the nature of the business and the assessed level of maturity required. There is also an ongoing need to consider if the organisation is delivering to the level of maturity.

This requires ongoing evaluation of effectiveness with a mindset on continual improvement. Every incident or reported failure to adhere to set requirements should be treated as an opportunity to evaluate the root cause and to improve the process.

Test and evaluation should be broad and regular to avoid falling into the common trap of feeling secure because an aspect of testing gives a good result.

THE 10 CYBER SECURITY MYTHS

Consider if you have heard the following myths being reported in your organisation. Organisations commonly mistake the 10 assertions below as evidence of adequate security.

MONITORING AND REPORTING

To date most organisations have focused on preventative controls such as firewalls, perimeter security, vulnerability testing, intrusion prevention etc. Security spend has been directed to these areas. As the nature of cyber-attacks become more sophisticated and time sensitive so the ability to prevent attacks from breaching an organisation's security reduces and the need to accept the notion of successful breaches. Hundreds of breaches occur daily in organisations spending significant amounts on security.

The security spend therefore needs to have a focus on the ability to monitor for breaches and to analyse the impact. This requires capability to perform the monitoring and actionable threat intelligence.

TOP 10 CYBER SECURITY MYTHS

1. **WE CONDUCT PENETRATION TESTS**

A penetration test is worthless unless the organisation manages and remediates the vulnerabilities it discovers. It is also important to consider the scope of the test; does it cover your whole infrastructure and simulate the most likely type of attack?

2. **WE HAVE INVESTED IN A HIGH-END SECURITY TOOL**

Security tools are only fully effective if they are correctly configured and appropriately monitored and maintained.

3. **WE COMPLY WITH INDUSTRY REGULATIONS AND BEST PRACTICES**

Compliance often requires only the bare minimum of security measures. Consider whether the compliance requirement is enough and the scope covers all your important systems and information. For example, is payment card data the only valuable data asset in your organisation?

4. **A THIRD-PARTY PROVIDER MANAGES OUR SECURITY**

Regardless of the provider's capabilities, it is critical you understand the threats to your organisation and how they are dealt with. Make sure your security provider is formally obliged to keep you informed of its security roles, responsibilities and processes.

5. **WE ONLY NEED TO PROTECT OUR INTERNET-FACING APPLICATIONS**

Protecting the internet-facing perimeter of an organisation is important, but should not be your only focus. You also need to have controls against malicious and accidental insider threats.

It is a well-known fact in the security industry that the multitude of threat information published daily is of little value unless it is relevant to the organisation and actionable by the organisation. The focus should be on gathering actionable intelligence.

POINTS TO CONSIDER

In today's world an appropriate response to a cyber incident or breach can mean the difference between success or failure of the organisation, the executives, the board or the CIO. In worse case scenarios we have seen the replacement of key executives and ongoing litigation.

The first step is to consider the cyber security capabilities required, given the nature of the business and the threats faced. Frameworks can help as a guide but the focus is on capability and services required, driven by the value of the information and how it is acquired and used rather than checklists.

6. WE HAVE NEVER BEEN ATTACKED, SO OUR SECURITY IS GOOD ENOUGH

Security threats are constantly growing in complexity and sophistication. A comprehensive security tool purchased two years ago may now be vulnerable to threats that emerged only last month.

7. SECURITY IS MANAGED BY THE IT DEPARTMENT AND IS NOT MY CONCERN

A security incident can have significant and long-lasting effects for the entire business. This is why it's important for business leaders and the IT department to manage cyber security together.

8. WE HAVE INVESTED IN STRONG SECURITY CONTROLS

It is not enough to focus on traditional IT security controls driven and prioritised by the IT team. To be effective, security investment needs to align with and secure critical business processes such as point-of-sale (PoS) devices, medical equipment and engineering systems.

9. WE ARE STATISTICALLY UNLIKELY TO EXPERIENCE A SECURITY BREACH

It is actually highly likely you will suffer a breach at some stage, so be prepared. Every organisation needs to be ready to respond to breaches quickly and have a plan for communicating the situation to customers and third parties so business can return to normal as quickly as possible.

10. WE HAVE COMPLETED OUR SECURITY PROJECT

Security is an ongoing process rather than an outcome. It is also something that should not be confined to a specific team or department. You need to embed cyber security measures into your organisation's key processes and invest in ongoing updates and monitoring to protect against newer, more elaborate attacks.

ARE YOU INSURED AGAINST CYBER RISKS?

Due to the evolving threats, every cyber or data loss incident is different in nature. No types of incidents are the same, with some requiring action and others no action. The incidents that pose the potential of serious risk/loss or compromise of data can have a very real impact on an organisation including significant financial implications and brand and market reputation damage.

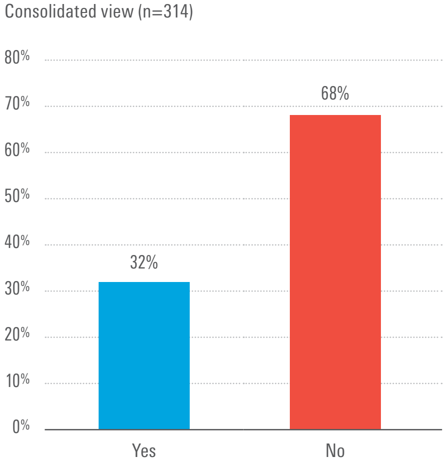
An interesting finding is the important role cyber insurance can play in not only managing the risk of a data breach but in improving the security posture of the company. While it has been suggested that having insurance encourages companies to slack off on security, the Ponemon Institute research suggests the exact opposite. Those companies with good security practices are actually more likely to purchase insurance.

Having adequate insurance in place that responds to the incident could be a major factor in recovering successfully from a cyber related incident. An organisation's existing insurance policies may provide some protection from cyber risks or data loss; however it's important to understand exactly what coverage, if any, is available under a current insurance program and how they interact with each other (i.e. in the event of a claim an organisation may be required to advise its insurer of other policies which may provide cover).

Understanding existing cover will enable an organisation to make informed decisions about risk transfer and determine which cyber liability insurance product best suits the organisation's risk profile and needs.

There are some points to consider when reviewing main existing insurance cover (there are a range of other insurance policies which may provide varying levels of cover, it's important to review these to understand what cover you have).

FIGURE 8. DOES THE ORGANISATION HAVE A DATA BREACH PROTECTION OR CYBER INSURANCE POLICY?



SOURCE: Deloitte.

In 2013 a major global retailer was cyber-attacked costing **MILLIONS OF DOLLARS** and **DRASTICALLY AFFECTING SHARE PRICES**.

1. BUSINESS INSURANCE POLICIES (BUSINESS PROPERTY)

It's important to understand that standard business insurance policies only cover 'tangible' assets, such as building and contents. Electronic data is not generally considered a tangible asset under standard business insurance policy definitions. Some policies may include an extension to include some 'loss of data' cover; however, generally sub-limits are applied. These sub-limits are typically too low to properly compensate for the loss and pay for the restoration of data.

2. PUBLIC AND PRODUCTS LIABILITY INSURANCE POLICIES (SOMETIMES REFERRED TO AS GENERAL LIABILITY)

This insurance cover may be a part of a business insurance policy (including covering buildings and contents), or as a stand-alone insurance policy. Unless specifically endorsed, this policy will generally exclude personal injury or property damage arising from your internet operations, and property damage to electronic data, computer programs or storage media.

3. PROFESSIONAL INDEMNITY

Some cover may be available under this policy; the nature of the cover available will depend on the specific policy wording, definitions and exclusions. It's important to note that some professional indemnity policies will exclude cybercrime.

What cover is available will generally relate to third party losses only, such as claims for compensation and damages. These third party losses however may be limited to exclude certain events, such as transmission of a virus through your computer system to a third party.

It's unlikely a professional indemnity policy will cover all losses to a business (first party losses). A professional indemnity policy may cover: defence costs; punitive fines and penalties; and court attendance. First party losses unlikely to be covered would include: data rectification costs; breach notification costs to your clients and customers; breach of an employee's data; loss of revenue; forensic investigation costs; and public relations expenses.

4. MANAGEMENT LIABILITY (INCLUDING DIRECTORS AND OFFICERS)

Similar to professional indemnity some cover may be available. The nature of the cover available will depend on the specific policy wording, extensions, definitions and exclusions. It's important to note that some management liability policies will exclude cybercrime, while other policies are offering to add cyber cover as an extension.

As with professional indemnity, the cover available will generally relate to third party losses and may be subject to specific exclusions and sub-limits. Again cover for first party losses may be limited.

CYBER INSURANCE – CONSIDERATIONS

Once an organisation has determined and understood the cover available under its existing insurance policies it is in a better position to purchase the type of cyber liability insurance that best suits its risk profile and needs.

The following are additional points to consider when either topping up an existing cover or looking to purchase additional cover.

1. IDENTIFY YOUR REAL UNIQUE RISKS

The initial step in purchasing cyber liability insurance is to understand the nature and the extent of the risks facing your organisation. Every organisation has a different risk profile based on the information that they manage and store. For banks and retailers, the primary concern would be the loss of personal identifiable information. In complete contrast, a utility or energy organisation faces a different risk, that being the disruption of critical businesses or physical operations through attacks on networks. **It is very important for organisations to tailor their cyber liability coverage to the direct risks that they face.**

2. PURCHASE WHAT YOU NEED

With the variety of products offered by insurers in the market, it is important to focus on the basics. Consider whether your organisation requires all the covers being offered and decline to purchase those that you do not need. Likewise, if an insurer is not willing to remove an objectionable exclusion or limitation from its policy, obtain quotes from an insurance carrier who will offer the coverage without the limitation. It is possible to design a policy and cover to suit your risk profile.

3. SECURE APPROPRIATE LIMITS AND SUBLIMITS

Perhaps the most important step an organisation can take to assess the value of cyber liability insurance is to compare the anticipated costs associated with a data breach (or security event) with limits of liability available and the related costs. The costs of responding to a data breach can be substantial. **Estimates vary, but in 2013 the average cost of a breach was $2.8 million, and the cost per lost electronic record was $145.** Your organisation should try to match its limits of liability with its realistic exposure in the event of a cyber loss. Also, most cyber liability insurance policies also impose sublimits on some cover, such as for crisis management expenses, notification costs and regulatory investigations. These sublimits are often inadequate, but many insurers are willing to negotiate on the size of the sublimit, often with no increase in premium.

4. BEWARE OF EXCLUSIONS

Often, cover for a loss or claim depends on the wordings in policy exclusion as opposed to the wordings in the grant of cover. As cyber liability insurance is a relatively new product, the policy wordings are not standardised. Policies may contain exclusions that have been cut and pasted from other insurance forms, and the exclusion simply may not belong.

5. GET RETROACTIVE COVERAGE

Cyber liability policies sometimes restrict coverage to breaches or losses that occur after a specific date. In some forms, this is the inception date of the policy. This means that there would be no coverage for breaches that occurred before the inception of the policy. Because breaches may go undetected for some period of time, it is important to purchase coverage with the earliest possible retroactive date.

6 CONSIDER COVERAGE FOR ACTS AND OMISSIONS BY THIRD PARTIES

Many organisations outsource data processing or storage to a third-party vendor. **It is important that your cyber liability insurance policy provides cover for claims that arise from misconduct by one of your vendors.**

7. EVALUATE COVERAGE FOR DATA RESTORATION COSTS

Many cyber liability insurance policies do not provide cover for the costs to replace, upgrade or maintain a computer system that was breached. Data restoration costs are potentially prohibitive. Any organisation that faces the risk of a data breach should take steps to ensure that its policies provide cover for the costs of putting the organisation back in the position it was in before the breach.

8. DOVETAIL CYBER INSURANCE WITH INDEMNITY AGREEMENTS

It is important that an organisation's indemnity agreements work hand-in-hand with its cyber liability insurance. For example, many cyber liability insurance policies have retentions and require that the retention be satisfied by the insured. Insurers may interpret this language to require that the insured pay the retention out of its own pocket and that a payment by a third party under an indemnity agreement would not satisfy the retention. This is a subject for negotiation with the insurer during the underwriting process.

9. UNDERSTAND THE 'TRIGGERS'

It is important to understand what activates cover under a cyber liability policy. Some policies are triggered on the date the loss occurs, while others are triggered on the date that a claim is made against the insured. In order to provide proper notice, understand how coverage applies under each policy purchased.

10. CONSIDER COVERAGE FOR LOSS OF INFORMATION ON UNENCRYPTED DEVICES

Many professionals today work on computers, smartphones and tablets outside the office. Although many organisations encrypt company-owned laptops, personally owned computers and storage devices are not. It is important for organisations facing a loss of data through personal computers to buy cyber liability insurance that provides cover for such losses.

11. CONSIDER COVERAGE FOR REGULATORY ACTIONS

A data loss may cause not only the loss of information, but also could result in regulatory actions against an organisation. Federal agencies have become more active in responding to data and privacy breaches. Consider whether your organisations cyber liability insurance policy provides cover for a regulatory investigation or a regulatory action arising from a cyber or data loss incident.

CYBER INSURANCE DOES NOT MEAN 'CYBER PREPARED'

Cyber liability insurance doesn't replace the need for: sound corporate controls; robust technology security systems; and vigilant regulatory compliance. Cyber liability insurance should be considered as an important component of any organisational risk management strategy in today's networked and cloud connected environment and considered as a pro-active risk mitigation investment.

Other aspects are to identify suitable companies to provide assistance when breaches do occur. These companies are experienced in conducting triage of breaches, evaluating what went wrong and conducting forensics.

The key point to move from reactive to proactive with these cyber-attacks is to have a Cyber preparedness plan in place, with safeguards in place, a plan that is established and tested with:

- Cyber crisis simulation to test incident response plans and prepare key stakeholders for an event
- Defined organisational cyber incident escalation matrices and roles and responsibilities
- A media response plan prepared and in place to respond to events as they occur
- Pre-contracted specialist resources such as forensic experts who are under a pre-existing contracted arrangement, have been involved in the preventative planning, understand your environment and can respond quickly to cyber-attacks, as part of incident response.

It is important that the employees responsible for cyber security identify the specialist resources needed to respond to cyber-attacks and create a standing contractual agreement to ensure an effective rapid response, and that the resources are engaged knowing the organisation's environment and customers.

Time is crucial in incident response, and an organisation doesn't want to be conducting contractual discussions where it will select a vendor without applying the usual selection processes, and end up paying a full premium for an urgent service as there are no other options.

The ultimate goal for an organisation is to move from a reactive to a proactive cyber security posture, by ensuring the right steps are in place to respond to cyber-attacks. The next one could happen to you, so ask the question of your organisation… are you cyber prepared?

The ultimate goal for an organisation is to move from a **REACTIVE TO A PROACTIVE CYBER SECURITY POSTURE**, by ensuring the right steps are in place to respond to cyber-attacks.

ROLE OF REGULATORS

DO REGULATORS HAVE A ROLE IN CYBER PREPAREDNESS?

While Australian and New Zealand regulators have cyber security strategies, their focus has not necessarily been on cyber preparedness. New Zealand released its updated Cyber Security Strategy in 2011 which detailed attempts to address three priority areas:

- Increasing awareness and online security.
- Protecting government systems and information.
- Incident response and planning.

Australia's Cyber Security Strategy was released in 2009 by the Attorney General's Department. It has three stated objectives:

- All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online.
- Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers.
- The Australian Government ensures its information and communications technologies are secure and resilient.

While these are important objectives, increasingly overseas regulators and governments are looking at the cyber preparedness of their regulated communities. Regulators in Australia and New Zealand have not been public in their statements about their role working with stakeholders on preparing for cyber threats. Nor has there been any co-ordinated effort across states and territories to manage regulations.

The key driver in Australia for ensuring cyber threats are addressed are via industry working on behalf of Australian Government, and some State and Territory Governments, who require industry to address cyber security only based upon policy and contractual requirements.

Even the Information Security Manual released by the Australian Signals Directorate (ASD) and Protective Security Policy Framework released by the Attorney-General's Department are regulated. Whilst provided in these documents, the ultimate responsibility is left to individual agencies to manage through their organisational risk appetite, and this is mostly left to the relevant agency to set, apart from the 'ASD Top 4' mitigations addressed earlier in this paper.

In many other countries regulators are actively meeting with chief executives to discuss cyber threats. In October 2014 the superintendent of New York's Department of Financial Services (DFS) said **'the cyber threat has to become urgent, one of the most important issues facing chief executives. It's got to be at chief executive level. It is not an IT problem.'**

The International Organisation of Securities Commissions (IOSCO) has stated that regulators are planning to introduce a global toolbox in 2015 that would be used to assess whether organisations are robust and managing their risks adequately in the event of a cyber attack. **The chairman of IOSCO has referred to cyber resilience as a sleeper issue and has predicted the next big financial shock will come from cyber space.**

The Securities Exchange Commission (SEC) in the United States has issued guidance to companies that have been the subject of a cyber attack. Both the SEC and the DFS are implementing specialised cyber preparedness examinations of the companies they regulate. This includes the SEC examining the cyber resilience of 50 broker-dealers and investment advisers. The Federal Bureau of Investigations (FBI) also meets frequently with financial industry representatives to help with their preparedness.

In 2014 the United Kingdom's Bank of England and Financial Conduct Authority (FCA) undertook a systemic survey of cyber resilience within the financial system. A number of organisations including the largest banks, investment firms, payment systems, clearing houses and exchanges completed a questionnaire on their cyber risk management practices. It allowed these regulators to evaluate cyber defences in individual organisations.

Following this initial questionnaire the Bank of England is now using a voluntary framework, CBEST, to test how regulated financial institutions are set to defend against cyber attacks. CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviours of different cyber threats, assessed by the UK government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions.

CONCLUSION

Recent high-profile security incidents resulting in data loss or system unavailability have raised awareness of the need for good cyber security.

The key for CIOs is to emphasise that cyber security is not about complying with regulation and investing in technology – it is about protecting the business along with its IP and sensitive information. Compliance should be part of information security, not the other way around.

Organisations must first consider the systems and information they value the most. These may include web-facing applications, personal data, or core network and storage components.

Having invested in the technology to protect these features, organisations need to ensure it is configured, maintained and monitored rigorously to strengthen the business against cyber-attacks.

Doing the bare minimum to pass compliance requirements is a common approach to cyber security, but fails to address the key risks and provide organisations with the core capabilities needed to protect their most valuable systems and information. Today's attack methods don't respect compliance frameworks. Capability is needed.

Accepting that cyber security is an ongoing challenge rather than a one-off achievement is the first step in ensuring your business is comprehensively secure. As for any business process, cyber security must be considered as a cyclic process as opposed to a linear activity and is continuous for the life of the organisation. It has no end.

> “…the cyber threat has to become urgent, one of the **MOST IMPORTANT ISSUES** facing chief executives.

THE SUPERINTENDENT
NEW YORK’S DEPARTMENT OF FINANCIAL SERVICES,
OCTOBER 2014.

REFERENCES

1. Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, May 2014
2. Symantec Corporation, *Internet Security Threat Report,* volume 19, April 2014
3. Australian Government, *Cyber Security Strategy*, 2009
4. New Zealand Government, *New Zealand's Cyber Security Strategy*, June 2011
5. Financial Times, *NY bank regulator targets cyber threat*, October 2014
6. Deloitte, *Global Executive Cyber Briefing*, 2014

Chartered Accountants Australia and New Zealand

Chartered Accountants Australia and New Zealand is made up of over 100,000 diverse, talented and financially astute professionals who utilise their skills every day to make a difference for businesses the world over.

Members of Chartered Accountants Australia and New Zealand are known for professional integrity, principled judgement, financial discipline and a forward-looking approach to business.

We focus on the education and lifelong learning of members, and engage in advocacy and thought leadership in areas that impact the economy and domestic and international capital markets.

We are a member of the International Federation of Accountants, and are connected globally through the 800,000-strong Global Accounting Alliance and Chartered Accountants Worldwide which brings together leading Institutes in Australia, England and Wales, Ireland, New Zealand, Scotland and South Africa to support and promote over 320,000 Chartered Accountants in more than 180 countries.

Chartered Accountants Australia and New Zealand is a trading name for The Institute of Chartered Accountants in Australia (ABN 50 084 642 571) and the New Zealand Institute of Chartered Accountants – see **charteredaccountantsanz.com** for further information.

About Deloitte

As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 6,000 people across the country. We have expertise that spans industry sectors including automotive; consumer business; energy and resources; financial services; government services; life sciences and health care; manufacturing; real estate; and technology, media and telecommunications. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. Our professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

DISCLAIMER This document was prepared by Chartered Accountants Australia and New Zealand with the assistance of Deloitte. The information in this document is provided for general guidance only and on the understanding that it does not represent, and is not intended to be, advice. Whilst care has been taken its preparation, it should not be used as a substitute for consultation with professional accounting, tax, legal or other advisors. Before making any decision or taking any action, you should consult with an appropriate specialist or professional.

Chartered Accountants Australia and New Zealand is a trading name for The Institute of Chartered Accountants in Australia (ABN 50 084 642 571) and the New Zealand Institute of Chartered Accountants – see **charteredaccountantsanz.com** for further information. 0914-106

CHARTERED ACCOUNTANTS
AUSTRALIA + NEW ZEALAND

future[inc]

A PLAN FOR AUSTRALIA + NEW ZEALAND'S PROSPERITY

charteredaccountantsanz.com/futureinc